REMARKS

Claims 1-46 were presented for examination and claims 1-46 were rejected. In the aforementioned amendment, claims 1, 3, 4, 6-10, 11, 12, 14, 17-20, 22, 24-28, 30, 33-35, 40, 45 and 46 have been amended, claims 36 and 41 have been canceled, and claims 47 and 49 have been added. Upon entry of the present amendment, claims 1-35, 37-40 and 42-48 will be presently pending in this application, of which claims 1, 17, 33, 34, 35, 40, 45 and 46 are independent claims. Applicants submit that claims 1-35, 37-40 and 42-48 are in condition for allowance.

The following comments address all stated grounds of rejection. Applicants respectfully traverse each rejection and urge the Examiner to pass the claims to allowance in view of the remarks set forth below.

Claim Amendments

Claims 36 and 41 have been canceled. Claims 1, 3, 4, 6-10, 11, 12, 14, 17-20, 22, 24-28, 30, 33-35, 40, 45 and 46 have been amended to clarify the scope of the claimed invention. Support for the amended claims can be found on page 3, lines 24-30 and throughout the remainder of the specification.

Dependent claims 47 and 48 have been added to more fully appreciate the scope of the claimed invention. Support for the added dependent claims can be found on page 11, lines 9-10 and throughout the remainder of the specification.

No new matter has been introduced. Applicants submit that the presently pending claims are in condition for allowance.

CLAIM REJECTIONS UNDER 35 USC §103

Claims 1-46 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Nessett et al. (US Patent No. 5,968,176) ("Nessett") in view of Dixon et al. (US Patent No. US 2003/0084331) ("Dixon"). For convenience of the discussion of the rejection by the Examiner to follow below, summaries of the claimed invention and the references cited in the rejection are described separately.

A. Summary of the Claimed Invention

The claimed invention is directed towards controlling a user's usage of network resources before a user can use any network resources beyond a network entry device. At the edge of the network, a network entry device provides connectivity between network resources and the user. A port module of the network entry devices provides connectivity for a user device to connect to the network entry device. To access network resources, the user device transmits one or more packets to the port module of the network entry device.

To control the user's use of network resources, the port module of the network entry device is configured with one or more packet rules corresponding to an identity of the user. As the port module receives packets from the user device, the port module applies the one or more packets rules to the received packets. As such, the port module of the network entry device is used to control the usage of network resources beyond the network entry device by the user. Thereby, no additional resources beyond this entry point are available to the user until the port module determines the packet received from the user should continue beyond the entry point in accordance with the packet rules.

B. Summary of Nessett

Nessett describes a system for establishing security in a network by distributing security functions across multiple protocol layers of multiple intermediate network devices to provide a pervasive firewall implementation. The purpose of the firewall implementation of Nessett is to improve security for activity originating inside the network. The firewall is pervasive in that it is distributed across multiple types of network devices with each network device type operating at a different protocol layer. Traditionally, firewalls are implemented in devices at network boarders to protect from activity originating from outside the network. However, as Nessett describes, corporations experience significant losses from activity occurring inside the network from insider attacks by disgruntled or opportunistic employees (see column 2, lines 12-16 of Nessett). Also, many corporations transact business electronically with external vendors through interior network devices (see column 2, lines 24-27 of Nessett). As such, corporations require security from attacks originating inside the network (see column 2, lines 19-30 of Nessett). Traditional border firewalls are unsuited to handle security for intermediate network activity as they are designed to protect against activity originating from outside the network (see column 2, lines 33-39 of Nessett). Nessett addresses intermediate network security requirements by distributing firewall functionality throughout many protocol layers of many different intermediate network devices (see column 2, lines 54-56 of Nessett).

Nessett also describes that distributing the firewall away from the borders across many network devices provides for better scalability of growing networks. This allows other network systems to handle firewall functionality rather than just the border systems as in a traditional firewall implementation. Additionally, Nessett distributes the firewall functionality at multiple network protocol layers such as the data link layer and the network layer. This provides a more

granular control of security than with traditional firewall functionality deployed at border devices (see column 3, lines 5-6 of Nessett).

C. Summary of Dixon

Dixon describes firewall functionality for providing a user security context for traffic from a user to an application. Dixon deploys this firewall functionality to an end computer system inside the network on the border of the network. This end computer system communicates with a network edge device, such as a gateway, through which a user accesses the network. Distributing firewall functionality to the end computer systems reduces the functions that intermediate network systems need to perform so that they can concentrate on faster network communications. As such, Dixon addresses network scaling and performance issues by deploying firewall functionality away from intermediate network devices to border systems (see page 1, paragraph 7, lines 1-9 of Dixon).

The firewall system of Dixon establishes the user security context through a secured socket based connection that links the user to the specific application. A user connects through a network edge device to the end computer system inside the network for authentication utilizing an encryption based security protocol. The user is authenticated to the end computer system by providing the appropriate digital certificate identifying the user. After the user is authenticated, the end computer system checks the user's authorization rights to access the application. If authorized, a specific secure socket connection is established between the user device and the application to provide a user security context. As such, the user security context is an application and device specific mechanism to establish an authorized flow of traffic. Thereafter, the user

device and the application exchange network traffic over the secure socket connection, which is an application to transport protocol network layer mechanism.

D. Claims 1-46 Distinguish Patentability over Nessett in view of Dixon

Claims 1-46 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Nessett in view of Dixon. Claims 36 and 41 are hereby canceled, mooting this rejection with respect to these claims. Claims 1, 17, 33, 34, 35, 40, 45 and 46 are independent claims. Claims 2-16 and 47-48 are dependent on claim 1, as amended, and, thus, incorporate the patentable subject matter of amended claim 1. Claims 18-32 are dependent on claim 17, as amended, and, thus, incorporate the patentable subject matter of amended claim 17. Claims 36-39 are dependent on claim 35, as amended, and, thus, incorporate the patentable subject matter of claim amended 35. Claims 41-44 are dependent on claim 40, as amended, and, thus, incorporate the patentable subject matter of amended claim 40. Applicants respectfully traverse this rejection and contend that Nessett in view of Dixon fails to detract from the patentability of claims 1-35, 37-40 and 42-48.

The Examiner cites Dixon for the purpose of suggesting that one ordinarily skilled in the art might modify Nessett to provide authentication of individual users. However, to establish a *prima facie* case of obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. Amended independent claims 1, 17, 33, 34, 35, 40, 45 and 46 are directed towards applying one or more packet rules at a port module of a network entry device to control usage, by the user, of any of the network resources. The packet rules are applied *before using, by the user, any of the network resources beyond the network entry device*. Nessett in view of Dixon does not teach or suggest controlling a user's usage of network resources *before using, by the user, any of the network resources beyond the network entry device*.

As discussed above, Nessett describes distributing firewall functionality to intermediate network devices for securing activity originating inside the network. Users connect to these devices inside the network after they have accessed the network beyond a network entry device. As such, the user has already consumed network resources beyond the network entry device and before the firewall functionality could control the user's use of such resources. Moreover, Nessett fails to describe controlling a user's usage of network resources *before using, by the user, any of the network resources beyond the network entry device.*

As discussed above, Dixon describes a user accessing an end computer system residing inside a network beyond a network edge device (see page 5, paragraph 46, lines 10-11 of Dixon). The network edge device is an entry point of the user to the network. The user connects beyond this network edge device to the end computer system to authenticate and access an application. In doing so, the user device exchanges network traffic with the end system. That is, network resources, for example, bandwidth and application resources, between the network edge device and the end computer system are consumed to facilitate this exchange. Therefore, the user uses network resources beyond the network entry device before the end system controls the user's usage of such resources. As such, Dixon fails to teach or suggest controlling a user's usage of network resources *before using, by the user, any of the network resources beyond the network entry device.*

Therefore, neither Nessett nor Dixon, alone or in combination, disclose, teach or suggest each and every element of claims 1-46.

Moreover, to establish a *prima facie* case of obviousness with which to reject Applicants' claimed limitations, there must be suggestion or motivation in the applied references, or in the knowledge of one ordinarily skilled in the art to modify the applied references. There is no

suggestion or motivation in the applied references, or in the knowledge of one ordinarily skilled in the art to combine Nessett in view of Dixon as suggested in the Office Action.

Dixon teaches away from Nessett. Nessett describes a firewall system distributed away from the border devices to intermediate network devices. The purpose of Nessett is to increase the functionality of intermediate network devices to handle firewall functionality for internal network activity (see column 2, lines 54-56 of Nessett). This allows the network to scale firewall functionality away from border devices to intermediate network devices (see column 2, lines 60-65 of Nessett). In contrast, Dixon describes a firewall system that is distributed to end systems near the network borders away from intermediate network devices (see page 1, paragraph 7, lines 5-8 of Dixon). Dixon scales firewall functionality to the end systems by reducing the firewall functionality deployed to intermediate network devices. This allows the intermediate network devices to focus on faster interior network communications (see page 1, paragraph 7, lines 8-15 of Dixon). Nowhere in Nessett or Dixon is there a motivation or suggestion to combine the teachings of these references. In fact, Dixon teaches away from Nessett and Nessett teaches away from Dixon with regards to machine dependent authentication.

As discussed above, Nessett distributes firewall functionality to multiple intermediate network devices operating at different protocol layers for more granular security control. That is, Nessett distributes firewall functionality using existing security features enforced in network devices operating at various protocol layers (see column 4, lines 21-24 of Nessett). The operation of these devices and the use of existing protocol layers is machine dependent. Since Nessett is directed towards securing activity originating inside the network, Nessett deals with users who have already gained authenticated access to the network and are consuming network resources. Thus, Nessett requires machine dependency to operate and is not concerned with the

authentication of individual users to the network. In contrast to Nessett, Dixon teaches user authentication to the network to provide a secured socket-based connection between the user and an application. Dixon teaches that current security protocols do not provide a mechanism to authenticate users as opposed to individual machines (see page 2, paragraph 10, lines 9-11 of Dixon). More specifically, Nessett requires the current security protocols that Dixon teaches away from. Therefore, nowhere in Nessett or Dixon is there a motivation or suggestion to combine these references.

Furthermore, the proposed combination of Nessett in view of Dixon would change the principle operation of Nessett. Combining the interior network firewall distribution of Nessett with the border firewall distribution of Dixon would result in a firewall implementation distributed through the entire network including both interior network devices and end systems. Since both the interior network devices and end systems are handling firewall functionality in the proposed combination, then neither the interior network devices nor the end systems are focusing on faster network communications. As such, the proposed combination would decrease performance and scalability of the network.

Additionally, modifying Nessett with the user security context mechanism of Dixon as the Examiner suggests would further change the principle operation of Nessett. As discussed above, Nessett distributes firewall functionality across various intermediate network devices operating at different protocol layers. In contrast, Dixon uses a secure socket-based connection to communicate specifically between the application and transport protocol layers of the network. This security mechanism cannot be applied to all the network devices of Nessett. Some devices of Nessett operate at protocol layers different than required by Dixon. Dixon's socket-based connection requires the transport protocol layer. A device in Nessett not supporting the transport

protocol layer, for example, a data link protocol layer device, cannot support socket connections as required by Dixon. Furthermore, security functionality at only a portion of the network protocol layers does not provide the granular control required by Nessett.

Even supporting the applicable protocol layers, such a proposed modification of Nessett in view of Dixon would significantly decrease the performance of the pervasive firewall implementation. With many intermediate network devices maintaining specific user to application socket connections, the network performance would significantly degrade managing the high volume of such connections.

Therefore, one skilled in the art would not find a motivation or suggestion to combine these references. Furthermore, the suggested combination of Nessett in view of Dixon would change the basic principle under which Nessett was designed to operate.

In light of the aforementioned arguments, Applicants contend that claims 1-35, 37-40 and 42-48 are patentable and in condition for allowance. Applicants therefore respectfully request the withdrawal of the Examiner's rejection of claims 1-35, 37-40 and 42-46 under 35 U.S.C. §103.

CONCLUSION

In view of the remarks set forth above, Applicants contend that claims 1-35, 37-40 and 42-48 presently pending in this application are patentable and in condition for allowance. Applicants respectfully urge the Examiner to pass the claims to allowance.

Respectfully submitted,
LAHIVE & COCKFIELD, LLP

Dated: June 8, 2004

By Christopher J. McKenna
Christopher J. McKenna
Registration No.: 53,302
Attorney/Agent For Applicant

Lahive & Cockfield, LLP
28 State Street
Boston, Massachusetts 02109
(617) 227-7400
(617) 742-4214 (Fax)